VŨ LÂM DANH

1050080130

10ĐH-CNPM2

**BÀI TẬP LAB 3**

Nguyên tắc hoạt động của Firewall Sophos UTM và Domain Controller trong mô hình mạng lab có thể được mô tả như sau dựa trên cách chúng tương tác và thực hiện chức năng trong một hệ thống mạng:

**1 Firewall Sophos UTM:**

◦ Firewall Sophos UTM hoạt động như một tường lửa bảo mật trung tâm, kiểm soát và quản lý toàn bộ lưu lượng mạng vào và ra khỏi hệ thống. Khi người dùng đăng nhập hoặc thực hiện các yêu cầu truy cập (ví dụ: truy cập website, gửi/nhận dữ liệu), thông tin của người dùng sẽ được gửi đến Sophos UTM.

◦ Tại đây, Sophos UTM kiểm tra các gói tin dựa trên các chính sách (rules) đã được thiết lập trước. Các chính sách này có thể bao gồm việc cho phép hoặc chặn truy cập dựa trên địa chỉ IP, giao thức, loại ứng dụng, hoặc danh mục nội dung (ví dụ: chặn mạng xã hội, website tìm việc).

◦ Sophos UTM sử dụng các tính năng như Network Protection (bảo vệ mạng khỏi tấn công), Web Protection (lọc URL và nội dung web), và Application Control (kiểm soát ứng dụng) để đảm bảo an toàn và tuân thủ chính sách mạng.

◦ Nguyên tắc hoạt động chủ đạo là phân tích lưu lượng mạng theo thời gian thực, áp dụng các quy tắc đã định nghĩa, và ngăn chặn các hành vi không được phép, từ đó bảo vệ mạng nội bộ khỏi các mối đe dọa từ bên ngoài hoặc bên trong.

**2 Domain Controller:**

◦ Domain Controller (DC) đóng vai trò là máy chủ quản lý tập trung trong mô hình mạng domain, chịu trách nhiệm xác thực và ủy quyền cho người dùng cũng như thiết bị trong hệ thống.

◦ Khi người dùng đăng nhập vào mạng, thông tin đăng nhập (username và password) sẽ được gửi đến Domain Controller. DC kiểm tra thông tin này trong cơ sở dữ liệu Active Directory để xác minh danh tính. Nếu hợp lệ, người dùng được cấp quyền truy cập vào các tài nguyên mạng (máy tính, tệp tin, ứng dụng) dựa trên vai trò và chính sách đã được gán.

◦ DC phối hợp với Firewall Sophos UTM bằng cách cung cấp thông tin xác thực người dùng, giúp Sophos áp dụng các chính sách phù hợp với từng tài khoản hoặc nhóm người dùng (ví dụ: cấm một số user truy cập mạng xã hội).

◦ Nguyên tắc hoạt động chính của DC là duy trì tính tập trung trong quản lý tài khoản và quyền truy cập, đảm bảo an ninh và đồng bộ hóa thông tin trong toàn bộ domain.

**Sự tương tác giữa Firewall Sophos UTM và Domain Controller:**

• Trong mô hình mạng lab, khi người dùng thực hiện một hành động (như truy cập Internet), Domain Controller xác thực danh tính người dùng trước, sau đó Firewall Sophos UTM sẽ kiểm tra yêu cầu dựa trên chính sách đã cấu hình cho user hoặc nhóm user đó.

• Hai thành phần này cùng nhau tạo thành một hệ thống bảo mật phân lớp: DC quản lý danh tính và quyền truy cập, còn Sophos UTM kiểm soát lưu lượng mạng và bảo vệ trước các mối đe dọa.